

PGP Corporate Desktop Privacy Products

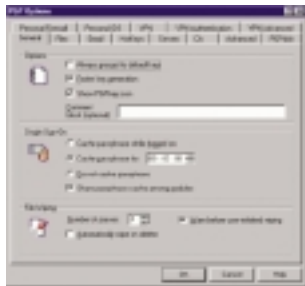
PGP Security, Protecting Your Privacy

Comprehensive, Enterprise Ready, Privacy Utilities For Individual Computers

PGP Security is a worldwide leader solving privacy and data confidentiality issues. Used by over 7 million people worldwide, PGP is the de facto encryption standard. PGP Corporate Desktop Privacy Products offer the four most critical security functions to protect information on individual computers, desktops and laptops. Each of the products is modularly defined and uses a common cryptosystem for key management and security functions. Each module can be installed selectively at any time to address security needs as they occur.

- **PGPdisk** – Storage privacy to protect your information in storage and to provide strong protection from unauthorized access
- **PGPmail/PGPfile/PGPicq** – Message privacy for email, file attachments and ICQ instant messaging.
- **PGPfire** – Firewall and Intrusion Detection protection to stop hackers and Trojan horses from entering the system and keep them out
- **PGPvpn** – IPsec Virtual Private Network (VPN) for private communications that extend your corporate network to SOHO and remote users

The PGP Corporate Desktop Privacy Products run on all major desktop platforms and provide the trusted personal security required for every employee's desktop and laptop computer.



PGP Corporate Desktop Privacy Products Offer the Four Most Critical Security Functions:

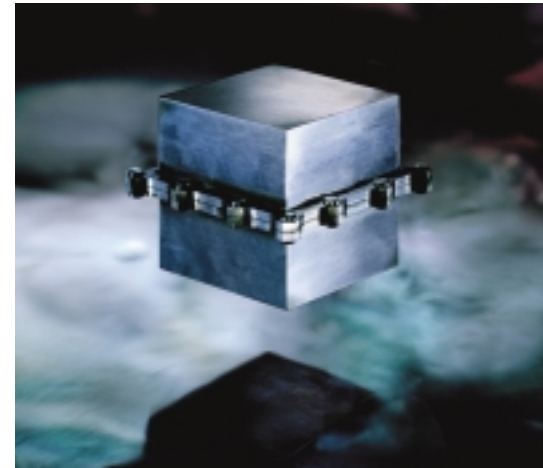
- Message Privacy
- Firewall and Intrusion Detection
- IPsec VPN
- Storage Privacy

PGPdisk: Secured Volume for Sensitive Data

Using PGP strong encryption methods, PGPdisk creates a secure volume to save your sensitive data. It provides fast and secure encryption for your data in encrypted files, which can be easily backed-up and exchanged with colleagues. SmartCard support offers two-factor security by requiring the device (Smart Card or Token) to be present in addition to the PGP passphrase authentication prior to decrypting the data.

PGPfile/PGPmail/PGPicq: Security for Files and Email attachments

PGPfile encrypts, decrypts, signs and verifies files for either email or secure storage on your computer. PGPicq secures instant messaging communication. PGPicq encrypts, decrypts, signs and verifies instant messages exchanged with over 41 million users worldwide. PGPwipe and Free Space Wiper functions delete files by erasing their content completely from your computer. With 70 percent of attacks occurring from inside corporate networks, the transparent encryption for all files ensures that the information on your computer is fully protected from unauthorized access.



Features and Benefits

PGPdisk/PGPmail

PGPfile/PGPicq

PGP Encryption

- PGP de facto strong encryption standard. Used by over 7 million people worldwide.
- Digital Signature for authentication and non-repudiation. The author is who he claims to be and cannot deny having sent the document.
- Self-Decrypting Archives (SDA). Share encrypted information with partners without encryption software.

PGPfire: Firewall and Intrusion Detection

- Complete control of inbound and outbound traffic. Select who accesses your computer, and how. Alerts you if your computer is under attack.

PGPvpn: Virtual Private Network

- To secure data sent over unsecured networks, such as the Internet. Your own private and secure connection.

*"PGP is an amazing product, as receipt of the Best Security Software top honor demonstrates. Security experts using security products in the real world [...] have awarded...] PGP as the best security solution on the market today."
- Paul Robinson, Publisher
SecureComputing Magazine*



A Network Associates Company

PGPfire—Personal Firewall Protection and Intrusion Detection

PGPfire checks data entering and leaving your computer based on filtering rules, protecting you from attacks that originate from within and outside the corporate network. PGPfire offers preset levels of protection and lets you define your own protection rules. If an intrusion event is detected, it records the event, the source address and the time it occurred, and alerts you of the attack.

PGPvpn—Virtual Private Network (VPN) Secure Connectivity

PGPvpn offers robust IPsec based VPN with IKE (Internet Key Exchange) aggressive mode and extended authentication support, enabling secure remote access. Administrators can disable the VPN portion of PGPvpn to use third-party VPN clients with other PGP Corporate Desktop Privacy Product modules.

VPN are required to securely send or receive data over an unsecured network, such as the Internet.

Protocols Supported:

- ICMP
- IGMP
- TCP
- UDP
- IPsec ESP
- IPsec AH

SmartCard and Token Support: Two-factor Security

Each module supports SmartCard technology devices offering the pkcs11 protocol and compatible with CAPI and PC/SC. This allows key pair generation on a SmartCard. The private key always remains on the SmartCard chip, even for decryption. The device, its PIN and the passphrase, are required to use the private key, providing two-factor security.

PGPadmin—Unmatched, Scalable Corporate Management

PGPadmin is included with each component and gives administrators complete control over enterprise deployment. Administrators can build deployment packages with policy

configuration predefined. They have the ability to cryptographically “lock down” policies so users cannot disable their privacy protection or break company policy. Each component has the ability to securely retrieve new policies from a central Lightweight Directory Access Protocol (LDAP) policy server.

PGP Encryption The De Facto Standard

The strong encryption and authentication capabilities available in all PGP Security products are provided by the PGP Cryptosystem available through the PGP Software Development Kit (PGPsdK). With the PGP Cryptosystem, PGP Security incorporates the world's most powerful security into each of its applications. Developers too can incorporate cryptographic capabilities into new or existing applications with the confidence that comes from using trusted and peer-reviewed PGP technology. PGPsdK provides a large number of operations through combinations of the following core functions:

- Generating and saving the user's key pair
- Retrieving the user's key pair
- Obtaining recipient's public key
- Generating a digital signature
- Verifying a digital signature
- Encrypting to a recipient's public key
- Decrypting with the user's private key

X.509 certificate support and IKE (Internet Key Exchange for IPsec) are also provided by PGPsdK in all PGP Security products. PGPsdK provides access to functions on LDAP key servers to search for, add, disable and delete keys on those servers. In addition, PGPsdK includes functions to connect to secure servers using TLS (Transport Layer Security, a protocol based on Secure Socket Layer (SSL)).

Algorithms Supported

Encryption Symmetric Key:

- 3DES
- CAST
- IDEA
- Twofish 256-bit
- AES up to 256-bit

Public Key Encryption:

- RSA v4 up to 4096-bit
- DSS
- Diffie-Hellman

Hash:

- SHA-1
- MD5

Messaging Platforms Supported

- Microsoft Outlook 97/98/2000
- Microsoft Outlook Express 4.x and 5.x
- Lotus Notes 4.5.x, 4.6.x and 5.0
- Qualcomm Eudora 4.x
- Claris Mailer for Macintosh

System Requirements

- Windows 95b/98/NT4.0 SP4+/2000/ME
- MacOS 8.6 or 9.x on PowerPC processor

All Platforms:

- 32 MB RAM and 12 MB disk space (for all components installed)

PGP Security Products

PGP Security, a Network Associates Company, protects your privacy through a full range of security products: Gauntlet Firewall/VPN, PGP Corporate Desktop Privacy Products, PGPwireless, CyberCop Scanner, E-Business Server, PGP Firewall/VPN e-appliances.

For more information on products, worldwide services, and support, contact your authorized PGP Security sales representative or visit us at:

3965 Freedom Circle
Santa Clara, CA 95054-1203
Tel (888) 747-3011
Fax (888) 203-9258

www.pgp.com



A Network Associates Company